ACTA ARITHMETICA
LXXVII.1 (1996)

Polars of Artin–Schreier curves

by

A. Hefez (Niterói) and N. Kakuta (S. José do Rio Preto)

1. Introduction. In this paper we study some properties of the special family of Artin–Schreier curves related to the theory of polar curves we developed in [2].

Our goal is to show how this theory can be carried out in concrete situations and also show how it can be used to determine new upper bounds for the number of rational points of projective plane curves over finite fields. The method we will employ to get such bounds is a generalization in some direction of the one introduced by Stöhr and Voloch in [4]. In general, our method gives better bounds than Weil's, essentially for curves of large degree with big genus (with respect to the degree). This is the case for example when the curve is smooth of large degree, so we could apply our method successfully to Fermat curves in [1]. However, an Artin–Schreier curve tends to have low genus with respect to its degree, moreover, it possesses a natural trivial bound, which is frequently better than Weil's and ours. Nevertheless, for these curves we still can improve in some cases all known upper bounds.

Throughout this paper we will use the notation of [2]. Let K be an algebraically closed field and let $Z : F = 0$ be a projective irreducible plane curve in $\mathbb{P}^2_K$ of degree d defined over K. Let λ be an integer such that $1 \le \lambda < d$, and some mixed Hasse derivative of order λ of F is not the zero polynomial. We have defined in [2] the λ-ic polar curve of Z at a point $P \in \mathbb{P}^2_K$ to be the curve $\Delta^\lambda_P Z$ defined by the zeros of the homogeneous polynomial

$$\Delta^\lambda_P F = \sum_{i_0+i_1+i_2=\lambda} (D_{i_0,i_1,i_2}F)(P) X_0^{i_0} X_1^{i_1} X_2^{i_2},$$

where D_{i_0,i_1,i_2} denotes the mixed Hasse differential operator of order i_ν with respect to each indeterminate X_ν, $\nu = 0, 1, 2$, respectively.

1991 *Mathematics Subject Classification*: Primary 14G15; Secondary 11G20.
The first author was partially supported by CNPq-Brazil.

In that paper we studied $I(P, Z.\Delta_P^\lambda Z)$, the intersection multiplicity function defined on Z, and showed that it is upper semicontinuous, with minimum value $\eta_{Z,\lambda}$ (achieved in an open dense Zariski subset of Z), and bounded from below by an arithmetical function $\eta(d,\lambda)$ (cf. [2]). When Z is a general curve of degree d it was shown that $\eta_{Z,\lambda} = \eta(d,\lambda)$, and in this case we say that Z is (d,λ)-*general*.

We will study in this paper, under the point of view of polars, the family of Artin–Schreier curves, which are the projective plane curves defined by affine equations of the form (1) below. The interest in studying such curves is that, first, they often appear in the literature as examples and test for conjectures, and secondly, they appear as central tools in several applications, as for example in the theory of cyclic codes, and in the theory of m-sequences.

The paper is organized as follows. In Section 2 we introduce the Artin–Schreier curves. In Section 3 we stratify all Artin–Schreier curves of a given degree d by the values of $\eta_{Z,\lambda}$, for certain values of λ, and describe through their equations the curves in each stratum. In Section 4 we introduce the notion of Frobenius degeneration, with respect to families of polars, and get upper bounds for the number of rational points, over a finite field, of the Frobenius non-degenerate curves in each stratum of the above stratification. In Section 5 we describe all Frobenius degenerate Artin–Schreier curves and show that these curves have the maximum allowed number of rational points. Section 6 is dedicated to present some examples.

2. Artin–Schreier curves. From now on, q will be a power of a prime number p. We will denote by $\mathbb{F}_q$ the finite field with q elements, and by K its algebraic closure.

The curves we are going to study in this paper are the projective plane curves Z in $\mathbb{P}^2_K$ defined by an affine equation of the form

$$f(x,y) = y^q + ay - \varphi(x) = 0, \tag{1}$$

where $a \in \mathbb{F}^*_{q^k}$ and $\varphi(x) \in \mathbb{F}_{q^k}[x]$, for some natural number k. Such curves are called *Artin–Schreier curves*.

We will restrict our attention to the case in which the degree d of $\varphi(x)$ is greater than q and less than q^k. When $d = q+1$, the projective closure of the curve is smooth, and when $d > q+1$, the curve has only one point at infinity which is its unique singular point. When d is prime to the characteristic, and the equation $T^q + aT = 0$ has all its roots in $\mathbb{F}_{q^k}$, then it is well known (cf. [5, Proposition VI.4.1]) that the curve is irreducible, it has the same number of rational points as its non-singular model, and its genus is given

by the formula

$$g = \frac{(d-1)(q-1)}{2}.$$

One can easily check that the number of rational points of Z over $\mathbb{F}_{q^k}$, denoted by $N(Z, q^k)$, is bounded from above by $q^{k+1}+1$, which we call the *trivial bound* for Artin–Schreier curves. When $N(Z, q^k) = q^{k+1}+1$, we say that Z has the *maximal number of rational points*.

We will give below a characterization of the Artin–Schreier curves with maximal number of rational points, for $a = \pm 1$ and $k = 2$.

Let $\mathcal{P}_a$ be the $\mathbb{F}_q$-endomorphism

$$\mathcal{P}_a : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}, \quad y \mapsto y^q + ay.$$

It is easy to check for $a = \pm 1$ that we have the equality

$$\mathrm{Im}(\mathcal{P}_a) = \mathrm{Ker}(\mathcal{P}_{-a}), \tag{2}$$

and these spaces are one-dimensional over $\mathbb{F}_q$.

PROPOSITION 2.1. *Let $a = \pm 1$ and let $Z : y^q + ay = \varphi(x)$ be defined over $\mathbb{F}_{q^2}$. The curve Z has the maximal number of rational points over $\mathbb{F}_{q^2}$ if and only if*

$$\varphi(c) \in \mathrm{Ker}(\mathcal{P}_{-a}), \quad \forall c \in \mathbb{F}_{q^2}. \tag{3}$$

P r o o f. If the curve has the maximal number of rational points, then for all $c \in \mathbb{F}_{q^2}$ the equation $y^q + ay = \varphi(c)$ has a solution, which in view of (2) implies (3).

On the other hand, suppose that (3) holds. Then in view of (2), for all $c \in \mathbb{F}_{q^2}$, the equation $y^q + ay = \varphi(c)$ has at least one solution in $\mathbb{F}_{q^2}$. Now it is easy to verify that for every solution $\alpha \in \mathbb{F}_{q^2}$, the q elements of the form $\alpha + \gamma$, with $\gamma \in \mathrm{Ker}(\mathcal{P}_a)$, are also solutions. This proves that Z has the maximal number of rational points over $\mathbb{F}_{q^2}$.

3. Non-general curves. In this section we will describe the Artin–Schreier curves which are not general with respect to the pair (d, λ), and determine the value of $\eta_{Z,\lambda}$.

If λ is an integer such that $1 \le \lambda < d$, it is easy to check that

$$D_{i,j}f = \begin{cases} a & \text{if } i = 0,\ j = 1, \\ 1 & \text{if } i = 0,\ j = q, \\ -D_x^i\varphi & \text{if } i \neq 0,\ j = 0, \\ 0 & \text{if } i = 0,\ j \neq 1, q \text{ or } ij \neq 0. \end{cases}$$

DEFINITION. We will say that the pair (d, λ) of integers is *admissible* if λ is equal to 1 or it is a truncation of the p-adic expansion of d.

If the pair (d, λ) is admissible, then it was shown in [2, Remark 1] that $\eta(d, \lambda) = \lambda + 1$.

We have the following result:

PROPOSITION 3.1. *Let $Z : f(x,y) = 0$ be defined as in* (1). *Suppose that $d \not\equiv 0 \bmod p$, or that the pair (d,λ) is admissible. Then the curve Z is not (d,λ)-general if and only if $\eta(d,\lambda) \neq q$ and $D_x^{\eta(d,\lambda)}\varphi = 0$.*

Proof. From [2, Theorem 2.5], Z is not (d,λ)-general if and only if

$$\Big(\sum_{r=0}^{\eta(d,\lambda)} D_x^r \circ D_y^{\eta(d,\lambda)-r} f\Big)(-f_x)^{\eta(d,\lambda)-r}(f_y)^r \equiv 0 \bmod f,$$

which in view of the expression of f is equivalent to

$$\binom{q}{\eta(d,\lambda)} y^{q-\eta(d,\lambda)}(-\varphi')^{\eta(d,\lambda)} - a^{\eta(d,\lambda)} D_x^{\eta(d,\lambda)}\varphi = hf, \tag{4}$$

where h is a polynomial in $K[x,y]$.

Note that

$$\binom{q}{\eta(d,\lambda)} \not\equiv 0 \Leftrightarrow \eta(d,\lambda) = q.$$

Hence, if $\eta(d,\lambda) \neq q$, we see from (4) that Z is not (d,λ)-general if and only if

$$-a^{\eta(d,\lambda)} D_x^{\eta(d,\lambda)}\varphi = hf.$$

Since the left hand side of the above equality depends only on x, and since $a \neq 0$, we must have $D_x^{\eta(d,\lambda)}\varphi = 0$.

If $\eta(d,\lambda) = q$, from (4) we see that Z is not (d,λ)-general if and only if

$$(-\varphi')^q - a^q D_x^q \varphi = hf,$$

which, by the same reason as above, is equivalent to

$$(-\varphi')^q = a^q D_x^q \varphi. \tag{5}$$

Now, if (d,λ) is admissible and $\eta(d,\lambda) = q$, it follows that $\lambda = q-1$, and therefore $d \equiv \lambda \not\equiv 0 \bmod p$. So in any case $d \not\equiv 0 \bmod p$, and consequently $\deg \varphi' = d-1$. But then, by degree reasons, (5) cannot be true, concluding thus our proof.

Let us define the integer ν as

$$\nu = \min\{i > \lambda \mid D_x^i \varphi \neq 0\}.$$

PROPOSITION 3.2. *Let $Z : f(x,y) = 0$ be defined as in* (1), *and suppose that the pair (d,λ) is admissible. Then*

$$\eta_{Z,\lambda} = \begin{cases} \nu & \text{if } \lambda \geq q, \\ \min\{q,\nu\} & \text{if } \lambda < q. \end{cases}$$

P r o o f. Let $P = (1; a; b)$ be a general point of the curve Z, and let $P' = (a, b)$. Since $\eta(d, \lambda) = \lambda + 1$, we know [2, (6)] that

$$\Delta^{\lambda}_{P'} f - \binom{d-1}{\lambda-1} f = - \sum_{r \geq \lambda+1} f_{r,P'}(x, y),$$

where

$$\Delta^{\lambda}_{P'} f = (\Delta^{\lambda}_{P} F)(1, x, y)$$

and

$$f_{r,P'}(x, y) = \sum_{i+j=r} D_{i,j} f(P')(x-a)^i (y-b)^j.$$

Defining

$$\varrho = \begin{cases} \nu & \text{if } \lambda \geq q, \\ \min\{q, \nu\} & \text{if } \lambda < q, \end{cases}$$

it follows from the formula for the derivatives of f that

$$\sum_{r \geq \lambda+1} f_{r,P'}(x, y) = \sum_{r \geq \varrho} f_{r,P'}(x, y),$$

hence,

$$\eta_{Z,\lambda} = I(P', f \Delta^{\lambda}_{P'} f) \geq \varrho.$$

On the other hand, choosing a parametrization of Z at P as follows:

$$P(t) = (1; a + t; b + b_1 t + b_2 t^2 + \ldots),$$

we have

$$\sum_{r \geq \varrho} f_{r,P'}(x(t), y(t)) = \sum_{r=0}^{\varrho} b_1^{\varrho - r} D_{r,\varrho-r} f(P') t^{\varrho} + \text{higher order terms in } t.$$

Suppose that $\eta_{Z,\lambda} > \varrho$. Then by an argument similar to the one we used in the proof of [2, Theorem 2.5], we have

$$\sum_{r=0}^{\varrho} (D_{r,\varrho-r} f)\, (f_y)^r (-f_x)^{\varrho-r} \equiv 0 \bmod f,$$

which by an argument similar to the one used in the proof of Proposition 3.1 implies that $\varrho \neq q$ and $D^{\varrho}_x \varphi = 0$ or $(-\varphi')^q = a^q D^q_x \varphi$. But the last case cannot happen by a degree argument, so $D^{\varrho}_x \varphi = 0$ and $\varrho \neq q$, a contradiction taking into account the definition of ϱ.

4. Bounds for rational points. As asserted in the introduction we will use the family of polar curves to determine upper bounds for the number of rational points of Artin–Schreier curves over finite fields. The method is described below.

Let $Z : F = 0$ be any plane projective curve defined over $\mathbb{F}_{q'}$, where q' is a power of p, and consider the Frobenius morphism

$$\mathcal{F}_{q'} : \mathbb{P}^2_K \to \mathbb{P}^2_K, \quad (X_0; X_1; X_2) \mapsto (X_0^{q'}; X_1^{q'}; X_2^{q'}).$$

Since $P \in \Delta_P^\lambda Z$ for all $P \in Z$ (see [2, Lemma 2.1(ii)]), and since the rational points of Z are the fixed points of the Frobenius morphism, it follows that the rational points of Z are among the points $P \in Z$ that satisfy the condition $\mathcal{F}_{q'}(P) \in \Delta_P^\lambda Z$.

If some mixed Hasse derivative of order λ of F is not zero then

$$H_\lambda(X_0, X_1, X_2) = \sum_{i_0+i_1+i_2=\lambda} (D_{i_0,i_1,i_2}F) X_0^{i_0 q'} X_1^{i_1 q'} X_2^{i_2 q'}$$

is a polynomial of degree $d - \lambda + \lambda q'$ such that

$$\mathcal{F}_{q'}(P) \in \Delta_P^\lambda Z \Leftrightarrow H_\lambda(P) = 0.$$

If H_λ does not vanish identically on Z, that is, if the polynomial F is not a divisor of H_λ, then the intersection set of the curves Z and $H_\lambda = 0$ is finite and contains the rational points of Z.

Suppose now that there exists an integer m such that for all rational points P of Z we have

$$I(P, F.H_\lambda) \geq m.$$

In fact, such an integer $m \geq 2$ exists and we will show that it is related to $\eta_{Z,\lambda}$.

If $N(Z, q')$ is the number of rational points of Z over $\mathbb{F}_{q'}$, then by Bézout's theorem,

$$N(Z, q') \leq d(d - \lambda + \lambda q')/m. \tag{6}$$

It is clear why the condition that F does not divide H_λ is important for the method to work. Therefore we give the following definition.

Definition. We say that a curve $Z : F = 0$ is λ-*Frobenius non-degenerate* if F is not a divisor of the polynomial H_λ. If the opposite holds, we say that Z is *Frobenius degenerate*.

In order to get concrete results from our theory, we must have easy-to-check criteria for the Frobenius non-degeneracy. This will be done for Artin–Schreier curves in Section 5.

The bound in (6) may be improved when the curve Z has singular or stationary rational points, since H_λ then vanishes to a higher order consuming more from the intersection of F and H_λ.

Let now $Z : F = 0$ be the projective plane curve in $\mathbb{P}^2_K$ of degree d with $q < d < q^k$, defined over $\mathbb{F}_{q^k}$ by the affine equation

$$f(x, y) = y^q + ay - \varphi(x) = 0$$

with $a \neq 0$, and let $q' = q^k$.

Let λ be an integer such that $1 \le \lambda < d$. We will express the polynomial H_λ, defined above, in terms of the mixed partial derivatives of f with respect to the indeterminates x and y. To do this, consider the following expression of the λ-ic polar, which can be found in [2, Lemma 2.4]:

$$\begin{aligned}\Delta_P^\lambda F &= X_0^\lambda \left[\Delta_P^\lambda F\left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right)\right] \\ &= X_0^\lambda \sum_{r=0}^{\lambda} a_0^{r-\lambda}\binom{d-r}{\lambda-r} \sum_{i+j=r} D_{0,i,j}F(P)\left(\frac{X_1}{X_0} - a\right)^i \left(\frac{X_2}{X_0} - b\right)^j.\end{aligned}$$

From this formula we find that H_λ is equal to

$$X_0^{\lambda q^k} \sum_{r=0}^{\lambda} X_0^{r-\lambda}\binom{d-r}{\lambda-r} \sum_{i+j=r} D_{0,i,j}F\left(\left(\frac{X_1}{X_0}\right)^{q^k} - \frac{X_1}{X_0}\right)^i \left(\left(\frac{X_2}{X_0}\right)^{q^k} - \frac{X_2}{X_0}\right)^j.$$

The dehomogenization of H_λ is then given by

$$h_\lambda = \sum_{r=0}^{\lambda} \sum_{i+j=r} \binom{d-r}{\lambda-r} D_{i,j}f(x^{q^k} - x)^i (y^{q^k} - y)^j.$$

We have the following result.

PROPOSITION 4.1. *Let $f(x, y) = 0$ be an Artin–Schreier curve as above, and let λ be an integer such that the pair (d, λ) is admissible. Then*

$$h_\lambda = \begin{cases} ay^{q^k} + y^q - \psi(x) & \text{if } \lambda < q, \\ y^{q^{k+1}} + ay^{q^k} - \psi(x) & \text{if } \lambda \ge q, \end{cases}$$

where

$$\psi(x) = \sum_{i=0}^{\lambda} (D_x^i \varphi)(x^{q^k} - x)^i \quad \text{with} \quad \deg \psi(x) = d - \lambda + \lambda q^k.$$

P r o o f. The proposition follows from the above expression of h_λ, where we replace the $D_{i,j}f$'s by their values and take into account the hypothesis on λ. Since (d, λ) is admissible, we get the equality for $\deg \psi$.

In order to study the intersection multiplicity of Z with the curve defined by $H_\lambda = 0$, at rational points, to get the upper bound for the number of such points, we will need the following notation and a lemma.

We will denote by U the set of rational points of Z at finite distance, that is,

$$U = Z(\mathbb{F}_{q^k}) \setminus \{P_\infty\}.$$

LEMMA 4.1. *For all integers m such that $m < q^k$, for all $P \in U$, and for*

$$\psi(x) = \sum_{i=0}^{\lambda} (D_x^i \varphi)(x^{q^k} - x)^i,$$

we have

$$D_x^m\psi(P) = c_m D_x^m\varphi(P), \quad \textit{where} \quad c_m = \sum_{i=0}^{\lambda}(-1)^i\binom{m}{i}.$$

P r o o f. First note that for all $P \in U$,

$$D_x^s(x^{q^k} - x)^i(P) = \begin{cases} (-1)^i & \text{if } s = i, \\ 0 & \text{if } s \neq i. \end{cases}$$

It follows, for all $P \in U$ and for all m with $1 \leq m < q^k$, that

$$\begin{aligned} D_x^m\psi(P) &= D_x^m\Big(\sum_{i=0}^{\lambda}(D_x^i\varphi)(x^{q^k} - x)^i\Big)(P) \\ &= \sum_{i=0}^{\lambda}\sum_{r+s=m}\binom{r+i}{i}D_x^{r+i}\varphi(P)(D_x^s(x^{q^k} - x)^i)(P) \\ &= \Big[\sum_{i=0}^{\lambda}(-1)^i\binom{m}{i}\Big]D_x^m\varphi(P) = c_m D_x^m\varphi(P). \end{aligned}$$

Corollary 4.1. *Notation as above. For all $P \in U$, we have*

$$D_x^m\psi(P) = 0, \quad \forall m;\ 1 \leq m < \nu.$$

P r o o f. This follows from the following obvious remarks. We have $c_m = 0$ if $1 \leq m \leq \lambda$, and $D_x^m\varphi = 0$ if $\lambda < m < \nu$.

We now give one of the crucial results of this section.

Proposition 4.2. *Let Z be an Artin–Schreier curve of degree d as above and let λ be an integer such that the pair (d, λ) is admissible. Then for all $P \in U$,*

$$I(P, Z.H_\lambda) \geq \eta_{Z,\lambda}.$$

P r o o f. Since $f_y = a \neq 0$, at every point P of U the function $t = x - x(P)$ is a local parameter of Z and consequently, for all $P \in U$,

$$I(P, F.H_\lambda) = \mathrm{ord}_t(h_\lambda) = \min\{s \mid D_x^s h_\lambda(P) \neq 0\}.$$

It is easy to verify that $D_x^m y^q = D_x^m y^{q^k} = 0$, $m = 1, \ldots, q-1$, and $D_x^q y^q = (D_x^1 y)^q$.

Suppose that $\lambda < q$. From the expression of h_λ in Proposition 4.1, from the above remarks, and from Corollary 4.1, we deduce that for all $P \in U$,

$$D_x^m h_\lambda(P) = 0, \quad \forall m = 1, \ldots, \min\{q, \nu\} - 1.$$

So the result is proved in this case in view of Proposition 3.2.

Suppose now that $\lambda \geq q$. In this case from the expression of h_λ in Proposition 4.1, we have $I(P, f.h_\lambda) = \min\{s \mid D_x^s \psi(P) \neq 0\}$, which by Lemma 4.1 is greater than or equal to ν, which in turn from Proposition 3.2 is equal to $\eta_{Z,\lambda}$.

LEMMA 4.2. *Let P_∞ be the point at infinity of the curve Z, and let λ be such that the pair (d, λ) is admissible. Then*

$$I(P_\infty, Z.H_\lambda) > \begin{cases} (d-q)[d-\lambda+(\lambda-1)q^k] & \text{if } \lambda < q, \\ (d-q)[d-\lambda+(\lambda-q)q^k] & \text{if } \lambda \geq q. \end{cases}$$

P r o o f. Homogenizing the expression of h_λ in Proposition 4.1, we see that H_λ is equal to

$$\begin{cases} aX_0^{d-\lambda+(\lambda-1)q^k} X_2^{q^k} + X_0^{d-\lambda+\lambda q^k-q} X_2^q - \Psi(X_0, X_1) & \text{if } \lambda < q, \\ X_0^{d-\lambda+\lambda q^k-q^{k+1}} X_2^{q^{k+1}} + aX_0^{d-\lambda+(\lambda-1)q^k} X_2^{q^k} - \Psi(X_0, X_1) & \text{if } \lambda \geq q, \end{cases}$$

where $\Psi(X_0, X_1)$ is the homogenization of the polynomial $\psi(x)$.

Since the equation of Z can be written as

$$F = X_0^{d-q} X_2^q + aX_0^{d-1} X_2 + \phi(X_0, X_1),$$

where $\phi(X_0, X_1)$ is the homogenization of the polynomial $\varphi(x)$, the multiplicity of Z at P_∞ is

$$m_{P_\infty}(Z) = d - q,$$

while the multiplicity of H_λ at P_∞ is

$$m_{P_\infty}(H_\lambda) = \begin{cases} d-\lambda+(\lambda-1)q^k & \text{if } \lambda < q, \\ d-\lambda+\lambda q^k-q^{k+1} & \text{if } \lambda \geq q. \end{cases}$$

Now since the curves Z and H_λ have the same tangent line at the point at infinity, we have

$$I(P_\infty, Z.H_\lambda) > m_{P_\infty}(Z).m_{P_\infty}(H_\lambda).$$

The result now follows from this inequality.

THEOREM 4.1. *Suppose that Z is Frobenius non-degenerate, and that the pair (d, λ) is admissible. Then*

$$N(Z, q^k) < \begin{cases} \dfrac{q^k[d+q(\lambda-1)]+q(d-\lambda)}{\eta_{Z,\lambda}} + 1 & \text{if } \lambda < q, \\ \dfrac{q^{k+1}[d+\lambda-q]+q(d-\lambda)}{\eta_{Z,\lambda}} + 1 & \text{if } \lambda \geq q. \end{cases}$$

P r o o f. Let $P_1, \ldots, P_N$ be the points of Z at finite distance and let P_∞ be the point at infinity of Z. Let $R = I(P_\infty, Z.H_\lambda)$. By Proposition 4.2,

$$\eta_{Z,\lambda}P_1 + \ldots + \eta_{Z,\lambda}P_N + \eta_{Z,\lambda}P_\infty + (R - \eta_{Z,\lambda})P_\infty \prec [F.H_\lambda],$$

where $[F.H_\lambda]$ is the intersection cycle of Z with the curve defined by $H_\lambda = 0$. Since Z is Frobenius non-degenerate, the result follows from Bézout's theorem and from Lemma 4.2.

Remark 1. Notice that the bound we got for $\lambda \geq q$ is useless because it is bigger than the trivial bound, since we always have $\eta_{Z,\lambda} < d + \lambda - q$.

Remark 2. Recall Weil's bound (see for example [5, V.2.3])

$$N(Z, q^k) \leq q^k + 1 + 2gq^{k/2}.$$

For $\lambda < q$, and $\eta_{Z,\lambda} = q$, it is easy to check that if our bound is simultaneously better than the trivial bound and Weil's bound then we must have $q < d < q^2$ and $k \leq 4$.

The above theorem can only be applied to Frobenius non-degenerate curves, therefore it is of fundamental importance to have criteria for Frobenius degeneration of curves. This will be done in the following section.

5. Frobenius degenerate curves. In this section we will characterize the Frobenius degenerate Artin–Schreier curves. Let Z be the curve with the affine equation

$$f(x, y) = y^q + ay - \varphi(x) = 0,$$

defined over $\mathbb{F}_{q^k}$ with $a \neq 0$, and $d = \deg \varphi < q^k$.

Proposition 5.1. *Let λ be a truncation of the p-adic expansion of d with $\lambda \geq q$. Then Z is λ-Frobenius non-degenerate.*

Proof. By Proposition 4.1, $h_\lambda = y^{q^{k+1}} + ay^{q^k} - \psi(x)$. On the other hand,

$$f^{q^k} = y^{q^{k+1}} + a^{q^k} y^{q^k} - [\varphi(x)]^{q^k} = y^{q^{k+1}} + ay^{q^k} - [\varphi(x)]^{q^k},$$

hence $h_\lambda = f^{q^k} + \varphi^{q^k} - \psi$. Therefore, if Z is λ-Frobenius degenerate then f divides $\varphi^{q^k} - \psi$, which is equivalent to $\varphi^{q^k} = \psi$. Computing the degrees in this expression, we conclude that $d - \lambda + \lambda q^k = dq^k$, hence $d = \lambda$, a contradiction.

Proposition 5.2. *Suppose that $a \in \mathbb{F}_q^*$, λ is such that the pair (d, λ) is admissible, and $\lambda < q$. Then Z is Frobenius degenerate if and only if $a = \pm 1$, $k = 2$, $d = \lambda(1 + q)$ and $\psi(x) = a[\varphi(x)]^q$, where $\psi(x)$ is as in Proposition* 4.1.

Proof. Since $a \in \mathbb{F}_q^*$, the affine equation of Z gives

$$\begin{aligned}(-1)^{k+1}a^{k+1}y + ay^{q^k} - [(-1)^{k-1}a^k\varphi + (-1)^{k-2}a^{k-1}\varphi^q + \ldots + a\varphi^{q^{k-1}}] \\ = (-1)^{k+1}a^k f + (-1)^{k-2}a^{k-1}f^q + \ldots + af^{q^{k-1}} \equiv 0 \bmod f.\end{aligned}$$

Hence

$$ay^{q^k} \equiv (-1)^k a^{k+1} y + [(-1)^{k-1} a^k \varphi + (-1)^{k-2} a^{k-1} \varphi^q + \ldots + a\varphi^{q^{k-1}}] \bmod f.$$

On the other hand, the affine equation of Z also gives

$$y^q \equiv -ay + \varphi(x) \bmod f.$$

It then follows that

$$\begin{aligned} h_\lambda &= ay^{q^k} + y^q - \psi(x) \\ &\equiv (-1)^k a^{k+1} y + [(-1)^{k-1} a^k \varphi + (-1)^{k-2} a^{k-1} \varphi^q + \ldots + a\varphi^{q^{k-1}}] \\ &\quad - ay + \varphi(x) - \psi(x) \bmod f. \end{aligned}$$

If Z is λ-Frobenius degenerate then

$$\begin{aligned} 0 \equiv\ & [(-1)^{k-1} a^{k+1} + a] y + \psi(x) - \varphi(x) \\ & - [(-1)^{k-1} a^k \varphi + (-1)^{k-2} a^{k-1} \varphi^q + \ldots + a\varphi^{q^{k-1}}] \bmod f, \end{aligned}$$

which implies that

$$\psi(x) - \varphi(x) - [(-1)^{k-1} a^k \varphi + (-1)^{k-2} a^{k-1} \varphi^q + \ldots + a\varphi^{q^{k-1}}] = 0 \tag{7}$$

and that

$$(-1)^{k-1} a^{k+1} + a = 0. \tag{8}$$

Comparing degrees in (7), we get $d - \lambda + \lambda q^k = dq^{k-1}$, which due to the condition $\lambda < q$ implies that $k = 2$ and $d = \lambda(1+q)$. Since (8) implies that $a^k = (-1)^k$, and since $k = 2$, we have $a = \pm 1$. It then follows from (7) that $\psi(x) = a\varphi(x)^q$.

Conversely, if $k = 2$ and $\psi(x) = a\varphi(x)^q$, then

$$h_\lambda = ay^{q^2} + y^q - a\varphi(x)^q = [ay^q + y - a\varphi(x)^q]^q.$$

It then follows, for $a = \pm 1$, that $h_\lambda = (\pm f)^q$. Therefore f divides h_λ, and consequently Z is λ-Frobenius degenerate.

Corollary 5.1. *Suppose that (d, λ) is admissible and $a \in \mathbb{F}_q^*$. If Z is Frobenius degenerate, then*

$$\varphi(c) = a\varphi(c)^q \quad \forall c \in \mathbb{F}_{q^2}.$$

Proof. From the expression of ψ it follows immediately that $\psi(c) = \varphi(c)$ for all $c \in \mathbb{F}_{q^2}$. Now the result follows from Proposition 5.2.

The following theorem generalizes one of the main results of [3], for Artin–Schreier curves.

Theorem 5.1. *Suppose that (d, λ) is admissible and $a \in \mathbb{F}_q^*$. If Z is λ-Frobenius degenerate, then Z has the maximal number of rational points.*

P r o o f. We know from Proposition 5.2 that if Z is Frobenius degenerate, then $k = 2, a = \pm 1$ and from Corollary 5.1, $\varphi(c) = a\varphi(c)^q$ for all $c \in \mathbb{F}_{q^2}$. Now the result follows from Proposition 2.1.

In order to find explicitly the equations of the Frobenius degenerate curves, we establish the following result.

PROPOSITION 5.3. *Let $\varphi(x) \in \mathbb{F}_{q^2}[x]$ with $\deg \varphi(x) < q^2$, and suppose that $a = \pm 1$. Write*

$$\varphi(x) = \sum_{i,j} a_{i+jq} x^{i+jq},$$

with $0 \le i, j < q$. Then

$$\varphi(c) = a\varphi(c)^q, \qquad \forall c \in \mathbb{F}_{q^2}, \tag{9}$$

if and only if

$$a_{i+jq} = a a_{j+iq}^q. \tag{10}$$

P r o o f. Condition (9) is equivalent to the fact that the polynomial

$$g(x) = \sum_{i,j} (a_{i+jq} - a a_{j+iq}^q) x^{i+jq}$$

defines the zero function on $\mathbb{F}_{q^2}$. Since $\deg g(x) < q^2$, this is equivalent to saying that $g(x)$ is the zero polynomial, which is equivalent to (10), proving the result.

COROLLARY 5.2. *Let $k = 2$, $a = \pm 1$ and $Z : y^q + ay = \varphi(x)$. Suppose that $\deg \varphi(x) < q^2$ and that Z has the maximal number of rational points. Then*

$$\varphi(x) = \sum_{i,j} a_{i+jq} x^{i+jq} \quad \text{with} \quad a_{i+jq} = a a_{j+iq}^q.$$

P r o o f. Proposition 2.1 yields that if Z has the maximal number of rational points, then (9) holds, which in view of Proposition 5.3 implies the result.

THEOREM 5.2. *Suppose that (d, λ) is admissible and $a \in \mathbb{F}_q^*$. The curve Z is λ-Frobenius degenerate if and only if $k = 2$, $a = \pm 1$, $d = \lambda(1 + q)$ and*

$$\varphi(x) = \sum_{0 \le i,j \le \lambda} a_{i+jq} x^{i+jq} \quad \text{with} \quad a_{i+jq} = a a_{j+iq}^q.$$

P r o o f. The "only if" assertion of the theorem follows from Corollary 5.1 and from Proposition 5.3.

Conversely, if $\varphi(x)$ is as above, then

$$\psi(x) = \sum_{k=0}^{\lambda} D_x^k \varphi(x) (x^{q^2} - x)^k$$

$$= \sum_{k=0}^{\lambda} \sum_{i,j} a_{i+jq} \binom{i}{k} x^{i+jq} (x^{q^2-1} - 1)^k$$

$$= \sum_{i,j} a_{i+jq} x^{i+jq} \sum_{k=0}^{\lambda} \binom{i}{k} (x^{q^2-1} - 1)^k$$

$$= \sum_{i,j} a_{i+jq} x^{jq+iq^2} = a \sum_{i,j} a_{j+iq}^q x^{jq+iq^2} = a[\varphi(x)]^q.$$

Therefore $\psi(x) = a\varphi(x)^q$ and from Proposition 5.2, the curve is λ-Frobenius degenerate.

It is not true that a curve of degree less than q^2 over $\mathbb{F}_{q^2}$ with the maximal number of rational points must be Frobenius degenerate. Here is an example:

$$y^q - y = x^{2+q} - x^{1+2q}.$$

6. Examples. We have seen in Remark 2 that there is a limitation for our method to improve simultaneously on Weil's bound and on the trivial bound, namely $q < d < q^2$, and $k \leq 4$.

In our examples we take $Z : y^q - y = \varphi(x)$ defined over $\mathbb{F}_{q^k}$, where $\varphi(x) = \sum_{i=0}^{d} a_i x^i$, with $q < d < q^2$. Write $d = \lambda + \alpha q$, with $0 \leq \lambda, \alpha < q$, and let λ_i be the remainder of the division of i by q. Suppose that

$$\lambda = \max\{\lambda_i \mid 0 \leq i \leq d\}.$$

It then follows from Proposition 3.2 that $\eta_{Z,\lambda} = q$. We will denote by N_λ the bound in Theorem 4.1, by N_{W} Weil's bound and by N_{T} the trivial bound.

Example 1. Here we assume $k = 2$. It is easy to verify that in this situation $N_\lambda \leq N_{\mathrm{W}}$, and if $\alpha + \lambda \leq q$, then $N_\lambda \leq N_{\mathrm{T}}$.

As a numerical example take $q = 81$, $k = 2$, $\lambda = 28$, $\alpha = 17$, and

$$Z : y^{81} - y = \sum_{i=0}^{17} x^{81i} P_i(x),$$

where each $P_i(x)$ is a polynomial in $\mathbb{F}_{q^2}[x]$ of degree at most 28. Then $\eta_{Z,\lambda} = 81$, and since $\alpha \neq \lambda$, by Proposition 5.2, Z is Frobenius non-degenerate. In this case we have $N_\lambda = 292{,}330$, $N_{\mathrm{T}} = 531{,}442$ and $N_{\mathrm{W}} = 9{,}104{,}482$.

Example 2. Here we take $k = 3$. In this case $N_\lambda < N_{\mathrm{T}}$ if $\alpha + \lambda \leq q$, and $N_{\mathrm{T}} < N_{\mathrm{W}}$ if $\alpha > \sqrt{q}$.

As a numerical example, take $q = 3^6 = 729$, $k = 3$, $\lambda = 50$, $\alpha = 45$ and

$$Z : y^{729} - y = \sum_{i=0}^{45} x^{729i} Q_i(x),$$

where each $Q_i(x)$ is of degree at most 50. It is clear that $\eta_{Z,\lambda} = 729$ and by Proposition 5.2, Z is Frobenius non-degenerate. In this case $N_\lambda = 36{,}344{,}056{,}922$ while $N_{\mathrm{T}} = 282{,}429{,}536{,}481$.

EXAMPLE 3. Here we take $k = 4$. It is easy to verify that when $\alpha + \lambda \leq q$ then $N_\lambda \leq N_{\mathrm{T}}$, and when $\lambda = 1$ and $\alpha \leq q - 2$, we have $N_\lambda < N_{\mathrm{W}}$.

As a numerical example, take $q = 9$, $k = 4$, $\lambda = 1$, $\alpha = 7$ and

$$Z : y^9 - y = x \sum_{i=0}^{7} a_i x^{9i}.$$

Then $\eta_{Z,\lambda} = 9$, and Z is Frobenius non-degenerate. In this situation $N_\lambda = 46{,}720$, $N_{\mathrm{W}} = 47{,}386$, and $N_{\mathrm{T}} = 59{,}050$.

References

[1] A. Hefez and N. Kakuta, *New bounds for Fermat curves over finite fields*, in: Proc. Zeuthen Sympos., Contemp. Math. 123, Amer. Math. Soc., 1991, 89–97.
[2] —, —, *Polar curves*, J. Algebra, to appear.
[3] A. Hefez and J. F. Voloch, *Frobenius non-classical curves*, Arch. Math. (Basel) 54 (1990), 263–273.
[4] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52 (1986), 1–19.
[5] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

Universidade Federal Fluminense
Departamento de Matemática Aplicada
R. São Paulo s/n
Campus do Valonguinho
24020-005 Niterói, RJ, Brazil
E-mail: gmahefe@vm.uff.br

Departamento de Matemática - IBILCE
R. Cristovão Colombo 2265
J. Nazareth
15054-000 S. José do Rio Preto, SP, Brazil
E-mail: neuza@condor.ibilce.unesp.br

Received on 19.9.1995 (2867)